UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,238	02/27/2002	Toru Mukai	2430-000001	2034

27572 7590 04/24/2006

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 04/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/084,238	**Applicant(s)** MUKAI ET AL.	
	Examiner Samson B. Lemma	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 January 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)□ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *4-35 and 38-60* is/are rejected.

7)□ Claim(s) *7-35 and 41-60* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *05/06/02 (5)*.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on January 11, 2006. **Claim 1-3, 36 and 37 have been canceled. Dependent Claims 58-60 have been Added. Therefore claims 4-35 and 38-60** are pending/examined. There are now two independent claims, namely claims 4 and 38.

Response to Arguments

2. Applicant's argument filed on January 11, 2006 have been fully considered but they are not persuasive.

Applicant's first argument is referring to the amended claim 4 which has the same limitation as that of independent claim 38. Applicant's argument is based on the amended claims and argued that the newly added limitation which is submitted is not suggested/discussed by **the reference** namely Schlossberg. Applicant wrote the following in support of his argument,

"Applicants' submit that claim 4 of the present invention describes "means for generating an image visualizing into respective objects" "a user using said devices", a device operating in said external network" and "communication conducted between each device inside and outside of said LAN". In contrast, paragraph 0076 and Fig. 9 of Schlossberg describes visualizing or indicating only intruder activities as 'blips' 915 while objects corresponding to "a user using said devices" and "communication conducted between each device inside and outside of said LAN" are not indicted. Therefore, Applicants invention as described in claim 4, displays objects differently from that disclosed in Schlossberg." Furthermore Applicant, made additional remark in support of his argument as follows,

" Applicants' note that claim 4 of the present invention involves three objects "a user using said devise", "a devise operating in said external network" , communication conducted between each device inside and outside of said LAN" are visualized and displayed simultaneously in a screen, and thus, an operator can find the situation inside and outside the LAN. On the other hand, according to Schlossberg, an operator can find only the intruder activities. Therefore, it is seen that the configuration according to Applicants' claim 4 is not described in Schlossberg.

Examiner disagrees with the above argument,

The argument raised by the applicant is what is already described by reference on the record, namely, Schlossberg reference.

In order to clarify the fact how each and every limitation of claim 4 is disclosed by the reference, the examiner would point out every limitation of the claims as follows. The amended Claim 4, recites the following limitation which is already disclosed by Schlossberg. Examiner asserts that **Schlossberg, discloses**,

A security administration server [figure 1, ref. Num "111, 115, 113, 117" and paragraph 0027] **installed in a predetermined LAN** [figure 1, ref. Num "120"; paragraph 0027](As disclosed on paragraph 0027, and shown on figure 1, the protected network/LAN 120, includes various segments/element/devices which elements that are grouped together "111, 115, 113, 117" met to be the administration server) **comprising**

Means for collecting information [paragraph 00053, figure 1, ref. Num "111" & "113", paragraph 0036-0038 and paragraph 0043, (As indicated on paragraph 0053, the receiving unit 111 shown on figure 1, 111 is the data collector among all other units in the network security system and As indication on paragraph

0043, deception units such as shown on figure 1, ref. 103, 105 and 109 in the system collects data from network traffic which is analyzed statically and the resulting information/collected information is transmitted to DBMS 113 data repository via the receiving unit 111, therefore the security administration server shown on figure 1 which includes unit 111 and 113 has a means for collecting information which has been collected by the deception devices) **relating to communication conducted via said LAN** [figure 1, ref. Num "120"] **by a device to be monitored** [paragraph 0043, figure 1, ref. "103, 105, and 109] **operating in said LAN** [figure 1, ref. Num "120"];

means for generating an image by extracting information useful for security management in said LAN from said collected communication related information and visualizing said information to a predetermined form:[paragraph 0055] (The purpose of the Watching Unit 115 shown in FIG. 1 ref. Num 115, which is part of the a security administrative server shown on figure 1, having the following component shown on figure 1, ref. Num "111", 113", "115" and "117" is to allow security management to view live data streams from any of the reporting units at. The Watching Unit 115 receives network security data from one or more of the DBMS unit 113, the Management Unit 117, the Reconnaissance Unit 121 and the Receiving Unit 111. The Watching Unit 115 provides graphic displays on a computer monitor and/or on print outs of pertinent security information, including but not limited to suspicious activities detected by the system, the current overall threat level facing the system, the past and/or real-time activities of an attacker (e.g., attempts to access a particular file or server), faults or points of vulnerability in the network, and information gathered on a particular attacker by the Reconnaissance Unit 121. By transforming the data gathered by the security system into graphics that can be rapidly comprehended by system security personnel, the Watching

Unit 115 improves the overall effectiveness of the security system by facilitating timely and effective operator intervention to appropriately respond to a particular threat or to conduct an investigation into an attack while it is occurring. An embodiment of one such graphical representation of threat data is more fully described below. This functionality is highly useful when an attack is in progress; it allows security management to watch a perpetrator's actions in real time. This capability allows security management to take immediate action when a breach in security has occurred.) **means for sending said image to a monitoring device wherein: [figure 1, ref. Num 150]** (Paragraph 0055) (The Watching Unit 115 provides graphic displays on a computer monitor meets the limitation of a monitoring device and/or on print outs of pertinent security information, including but not limited to suspicious activities detected by the system, the current overall threat level facing the system, the past and/or real-time activities of an attacker (e.g., attempts to access a particular file or server), faults or points of vulnerability in the network, and information gathered on a particular attacker by the Reconnaissance Unit 121).

Said LAN [Figure 1, ref. Num "120"] is connected to an external network such as the Internet [figure 1, ref. Num "160"], and

said image generating means comprises [figure 1, ref. Num "115", paragraph 0055] **means for generating an image visualizing into respective predetermined objects simultaneously [Paragraph 0055]**(By transforming the data gathered by the security system into graphics that can be rapidly comprehended by system security personnel, the Watching Unit 115 improves the overall effectiveness of the security system by facilitating timely and effective operator intervention to appropriately respond to a particular threat or to conduct an investigation into an attack while it is occurring means the limitation of "visualizing into respective predetermined objects simultaneously.), **said device to be monitored,**[figure 1, ref. Num "103", 105 and 109] **a device operating in said external network which communicates with said device to be monitored** [figure 1, ref. Num "121"; paragraph 0055], **a user using said devices** [paragraph 0055 and 0060, see "security personnel"] (By transforming the data gathered by the security system into graphics that can be rapidly comprehended by system security personnel/user, the Watching Unit 115 improves the overall effectiveness of the security system by facilitating timely and effective operator/user intervention to appropriately respond to a particular threat or to conduct an investigation into an attack while it is occurring)**, and communication conducted between said devices inside and outside of said LAN.[figure 1 and paragraph 0055 and 0060, abstract]** (the communication is conducted between the device to be monitored such as devices shown on figure 1, ref. 103, 105 and 109 and a device operating in said external network as shown on figure 1, ref. Num "121" which communicates with said device to be monitored shown figure 1, ref. 103, 105 and 109, and explained on paragraph 0055 & 0060 and user using such device/operator shown on figure 1, ref. Num "150" and explained on paragraph 0055 and 0060 and communication conducted between said devices inside and outside of said LAN as shown on figure 1 or paragraph 0055 and 0060 or abstract]

Therefore, as examiner explained above each and every limitations of the amended claim is disclosed by the reference on the record, namely **Schlossberg**.

The second argument made by the applicant is referring to dependent claims 5 and 6. Applicants note that Schlossberg does not describe dividing into groups said objects according to **a predetermined standard** and visualizing each group in layers. Further, the predetermined standard for grouping is based on reliability between each device and LAN which is not recited or contemplated by Schlossberg.

Examiner disagrees with the above argument and points out that, the argument raised by the applicant is based on the term "predetermined standard" which is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 5 and 39 recites the term "predetermined standard." This term is vague and is subjected to change and does not have a clear and well defined meaning. It has to be explicitly defined to be considered. For the same of examination, examiner interprets the term "predetermined standard" as "predetermined value". However applicant needs to provide the exact term which is supported by the specification.

The rest of the limitation in these claims 5-6 and 39-40 are disclosed by the reference on the record and this is shown as follows.

Schlossberg discloses a security administration server as applied to claims above. Furthermore Schlossberg discloses said image generating means [paragraph 0055, "watching unit generating image"] **comprises means for dividing in groups** [figure 9, ref. Num "911"/DMZ, Finance and Engineering group] **or said object [figure 9, ref. Num "917" and "919" and figure 4, "threat level"] according to a predetermined values** [figure 4, ref. "pre-determined time elapsed window]**, and for a generating an image visualizing each group in layers.**[figure 4 and figure 9]

Therefore each and individual limitation of the independent claims is disclosed by the reference on the record. The rejection remains to be valid, unless and otherwise the claims are amended and overcome the ground of rejection set forth in the office action without introducing new matter.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claim 4 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Based on a thorough review of the entire disclosure and a text search for "simultaneously", there is no "readily apparent support" how the three objects "a user using said device", "a device operating in said external network" and communication conducted between each device inside and outside of said LAN are visualized and displayed simultaneously in a screen. Therefore the examiner does not see support for the amended limitation in particular "Simultaneously".

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. **Independent Claim 4 i**s rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 recites the term "said device" at lines 11, 12, 13 and 14 of claim 4. There are two different devices which are indicated in the limitation prior to these references. The first one which is indicated on line 4, "a device to be monitored" and the second one which is indicated on line 8 referring to

monitoring device. It is not only vague but also ambiguous to know which one is referred by "**said device**". If they are one and the same device, applicant has to also explicitly and clearly indicate it in the limitation otherwise each one of them has to be written and referred to distinctively to avoid ambiguity. Besides on line 13 of claim 4, "said deice" is recited, (Spelling error) it is not clear whether or not it is referring to which "device".

7. **Independent Claim 38 i**s rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 38 recites the term "said device" at lines 12 and 13. There are two different devices which are indicated in the limitation prior to these reference. The first one which is indicated on line 5 of claim 38, as means for passively and actively collecting log information stored and managed **by a device operating in said LAN** and the second one which is indicated on line 9 referring to **another device.** It is not only vague but also ambiguous to know which one is referred by "**said device**". Each one of them has to be written and referred to distinctively to avoid ambiguity.

8. **Dependent Claims 5-6 and 39-40 are** rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 5-6 and 39-40 recites the term "predetermined standard." This term is vague and is subjected to change and does not have a clear and well defined meaning. It has to be explicitly defined to avoid ambiguity. For the purpose of examination examiner interprets the term "predetermined standard" as a "predetermined value".

9. **Claims 7-35 and 41-60** depend from the rejected claims 4-6 and 38-40, and include all the limitations of the respective claims, thereby rendering those dependent claims indefinite.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. **Claims 4-6 and 36-40** are rejected under 35 U.S.C. 102(e) as being anticipated by **Schlossberg et al.** (hereinafter referred as **Schlossberg**) (U.S. Publication No. 2002/0066034) which claims the priority of provisional application No. 60/242675 filed on Oct 24, 2000)

12. **As per claims 4 and 38 Schlossberg discloses a security administration server** [figure 1, ref. Num "111, 115, 113, 117" and paragraph 0027] **installed in a predetermined LAN** [figure 1, ref. Num "120"; paragraph 0027](As disclosed on paragraph 0027, and shown on figure 1, the protected network/LAN 120, includes various segments/element/devices which elements that are grouped together "111, 115, 113, 117" met to be the administration server) **comprising**

Means for collecting information [paragraph 00053, figure 1, ref. Num "111" & "113", paragraph 0036-0038 and paragraph 0043, (As indicated on paragraph

0053, the receiving unit 111 shown on figure 1, 111 is the data collector among all other units in the network security system and As indication on paragraph 0043, deception units such as shown on figure 1, ref. 103, 105 and 109 in the system collects data from network traffic which is analyzed statically and the resulting information/collected information is transmitted to DBMS 113 data repository via the receiving unit 111, therefore the security administration server shown on figure 1 which includes unit 111 and 113 has a means for collecting information which has been collected by the deception devices) **relating to communication conducted via said LAN** [figure 1, ref. Num "120"] **by a device to be monitored** [paragraph 0043, figure 1, ref. "103, 105, and 109] **operating in said LAN** [figure 1, ref. Num "120"];

means for generating an image by extracting information useful for security management in said LAN from said collected communication related information and visualizing said information to a predetermined form:[paragraph 0055] (The purpose of the Watching Unit 115 shown in FIG. 1 ref. Num 115, which is part of the a security administrative server shown on figure 1, having the following component shown on figure 1, ref. Num "111", 113", "115" and "117" is to allow security management to view live data streams from any of the reporting units at. The Watching Unit 115 receives network security data from one or more of the DBMS unit 113, the Management Unit 117, the Reconnaissance Unit 121 and the Receiving Unit 111. The Watching Unit 115 provides graphic displays on a computer monitor and/or on print outs of pertinent security information, including but not limited to suspicious activities detected by the system, the current overall threat level facing the system, the past and/or real-time activities of an attacker (e.g., attempts to access a particular file or server), faults or points of vulnerability in the network, and information gathered on a particular attacker by the Reconnaissance Unit

121. By transforming the data gathered by the security system into graphics that can be rapidly comprehended by system security personnel, the Watching Unit 115 improves the overall effectiveness of the security system by facilitating timely and effective operator intervention to appropriately respond to a particular threat or to conduct an investigation into an attack while it is occurring. An embodiment of one such graphical representation of threat data is more fully described below. This functionality is highly useful when an attack is in progress; it allows security management to watch a perpetrator's actions in real time. This capability allows security management to take immediate action when a breach in security has occurred.) **means for sending said image to a monitoring device [figure 1, ref. Num 150] wherein,** (Paragraph 0055) (The Watching Unit 115 provides graphic displays on a computer monitor meets the limitation of a monitoring device and/or on print outs of pertinent security information, including but not limited to suspicious activities detected by the system, the current overall threat level facing the system, the past and/or real-time activities of an attacker (e.g., attempts to access a particular file or server), faults or points of vulnerability in the network, and information gathered on a particular attacker by the Reconnaissance Unit 121). **said LAN [Figure 1, ref. Num "120"] is connected to an external network such as the Internet** [figure 1, ref. Num "160"], and

said image generating means comprises [figure 1, ref. Num "115", paragraph 0055] **means for generating an image visualizing into respective predetermined objects simultaneously [Paragraph 0055]**(By transforming the data gathered by the security system into graphics that can be rapidly comprehended by system security personnel, the Watching Unit 115 improves the overall effectiveness of the security system by facilitating timely and effective operator intervention to appropriately respond to a particular threat or to conduct an investigation into an attack while it is occurring means the limitation of "visualizing into respective predetermined objects simultaneously.), **said device to be monitored,**[figure 1, ref. Num "103", 105 and 109] **a device operating in said external network which communicates with said device to be monitored** [figure 1, ref. Num "121"; paragraph 0055], **a user using said devices** [paragraph 0055 and 0060, see "security personnel"**]** (By transforming the data gathered by the security system into graphics that can be rapidly comprehended by system security personnel/user, the Watching Unit 115 improves the overall effectiveness of the security system by facilitating timely and effective operator/user intervention to appropriately respond to a particular threat or to conduct an investigation into an attack while it is occurring)**, and communication conducted between said devices inside and outside of said LAN.[figure 1 and paragraph 0055 and 0060, abstract]** (the communication is conducted between the device to be monitored such as devices shown on figure 1, ref. 103, 105 and 109 and a device operating in said external network as shown on figure 1, ref. Num "121" which communicates with said device to be monitored shown figure 1, ref. 103, 105 and 109, and explained on paragraph 0055 & 0060 and user using such device/operator shown on figure 1, ref. Num "150" and explained on paragraph 0055 and 0060 and communication conducted between said devices inside and outside of said LAN as shown on figure 1 or paragraph 0055 and 0060 or abstract]

13. **<u>As per claims 5-6 and 39-40</u> Schlossberg discloses a security administration server as applied to claims above. Furthermore Schlossberg discloses said image generating means** [paragraph 0055, "watching unit generating image"**] comprises means for dividing in groups** [figure 9, ref. Num "911"/DMZ,

Finance and Engineering group] **or said object [figure 9, ref. Num "917" and "919" and figure 4, "threat level"] according to a predetermined values** [figure 4, ref. "pre-determined time elapsed window]**, and for a generating an image visualizing each group in layers.**[figure 4 and figure 9]

Allowable Subject Matter

14. **Claims 7-35 and 41- 60** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Samson Lemma
S. L.
March 26, 2006

Gilberto
GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100